REMARKS

Claims 1-10, 12, 13, 15-17, 19, 21 and 22 are currently pending in the subject application and are presently under consideration. Claims 1, 12, 15, 19, 21 and 22 have been amended as shown at pages 2-6 of the Reply. Claim 19 has been cancelled.

Applicants' representative thanks Examiner Traore for the courtesies extended during the telephonic interview conducted on July 15, 2008. Examiner was contacted to discuss the claim rejections under 35 U.S.C. §112, 35 U.S.C. §101 and 35 U.S.C. §103(a). During the interview a set of proposed amendments were agreed upon that addressed all of the claim rejections under 35 U.S.C. §112 and 35 U.S.C. §101 identified in the Office Action. These amendments have been incorporated into the claims as shown above. Additionally, proposed amendments were presented to provide additional clarity and overcome the rejections in view of cited art. Examiner indicated that further search and consideration was required to determine if the claims would be allowed over the cited prior art.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1, 12, 21 and 22 Under 35 U.S.C §112

Claims 1, 12, 21 and 22 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 1, 12, 21, and 22 have been amended to provide additional clarity. As such, this rejection should be withdrawn.

II. Rejection of Claims 1-10 and 19 Under 35 U.S.C. §101

Claims 1-10 and 19 stand rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. Independent claim 1 has been amended to address this rejection. Claim 19 has been cancelled. Accordingly, withdrawal of this rejection is respectfully requested.

III. Rejection of Claims 1-3, 19, 21 and 22 Under 35 U.S.C. §103(a)

Claims 1-3, 19, 21 and 22 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Ayyagari, *et al.* (US 2002/0176366) in view of He, *et al.* (US 6,088,451). It is respectfully

submitted that this rejection should be withdrawn for at least the following reasons. Ayyagari, *et al.* and He, *et al.* does not teach each and every element of applicants' invention as recited in the subject claims.

> A factfinder should be aware, of course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon *ex post* reasoning. See *KSR v. Teleflex*, 550 U.S. ___, 127 S. Ct. 1727 (2007) citing Graham v. John Deere Co. of Kansas City, 383 U. S. 1, 36 (warning against a "temptation to read into the prior art the teachings of the invention in issue" and instructing courts to "'guard against slipping into the use of hindsight'" (*quoting Monroe Auto Equipment Co. v. Heckethorn Mfg. & Supply Co.*, 332 F. 2d 406, 412 (CA6 1964))).

The subject claims relates to identification of the type of security encryption employed on a wireless network, for example, by detecting failures and timeouts during authentication. By recognizing failures or timeouts during particular portions of the authentication process, an iterative approach can narrow down the possible encryption types until identification of the encryption type being employed is achieved, without any user input or pre-stored information regarding the network encryption type. In particular, independent claim 1 (and similarly independent claim 21) recites *a connection component that can connect a device to a plurality of wireless networks; and, a detection component that automatically* ***identifies an encryption type of an available wireless network****, wherein* ***identification of the encryption type is based at least in part upon eliminating one or more of a plurality of possible encryption types by at least one of detecting a failure of a portion of an authentication sequence of the available wireless network or exceeding a time threshold without having detected an expected portion of the authentication sequence of the available wireless network, wherein identifying the encryption type includes: the detection component attempting an 802.1x authentication sequence to the wireless network and determining that the wireless network as a wired equivalent privacy network requiring a wired equivalent privacy key when a failure of a portion of the 802.1x authentication sequence or exceeding a time threshold without having detected an expected portion of the 802.1x authentication sequence occurs; the detection component identifying the wireless network as a 802.1x when a failure of a portion of the 802.1x authentication sequence and exceeding a time threshold without having detected an expected portion of the 802.1x***

authentication sequence do not occur; the detection component having identified the wireless network as a 802.1x attempting a wireless provisioning services sequence and determining that the wireless network does not support wireless provisioning services when the wireless network supports 802.1x when a failure of a portion of the wireless provisioning services authentication sequence or exceeding a time threshold without having detected an expected portion of the wireless provisioning services authentication sequence occurs; and, the detection component identifying the wireless network as a 802.1x supporting wireless provisioning services network when no failure of a portion of the wireless provisioning services authentication sequence and exceeding a time threshold without having detected an expected portion of the wireless provisioning services authentication sequence do not occur.

As conceded in the Office Action dated April 21,2008, Ayyagari, *et al.* does not teach or suggest the aforementioned novel features as recited in the subject claims. The cited reference discloses a system for switching between available networks as a user moves to different locations without the user having to manually enter network connection information upon arrival at each location. This is accomplished by the system caching information when a user enters information the first time or providing a UI for the user to enter information for networks in advance as stored network preferences. The system employs beacon information received/downloaded from the network to identify available networks and uses the cached or stored information to connect to the known networks. If there are no known networks the system attempts to connect to ad hoc networks. When the system attempts to connect to a network and the connection fails, the system attempts to connect to a different network. Ayyagari, *et al.* does not teach identifying the encryption type of a wireless network by eliminating one or more of a plurality of possible encryption types by at least one of detecting a failure of a portion of an authentication sequence of the available wireless network or exceeding a time threshold without having detected an expected portion of the authentication sequence of the available wireless network. He, *et al.* is cited to make up for this deficiency of Ayyagari, *et al.* On the contrary, He, *et al.* discloses a system for managing secured access to network resources using a general ticket that is issued upon a first authentication of the user and is reused for subsequent requests. The cited section refers to use of a Kerberos authentication security as the general ticket server for a dial-up server. Upon a failure of the Kerberos server or a server timeout, the system switches the user to a dial-up access to the network. In this scenario the security mechanisms are

known to the server and there is no identification of encryption types being performed. Moreover, He, *et al.* is concerned with hardwired network security. The reference is silent regarding wireless networks or identification of encryption types on a wireless network. As such, He, *et al.* is completely unrelated to the features subject claim and fails to make up for the deficiencies of Ayyagari, *et al.* Therefore, Ayyagari, *et al.* and He, *et al.* fail to teach or suggest the specific sequence of detection identified in the subject claim.

Furthermore, independent claim 22 recites *means for connecting a device to a plurality of wireless networks; and, means for automatically* ***identifying an encryption type of an available wireless network****, wherein identification of the encryption type is based at least in part upon* ***eliminating one or more of a plurality of possible encryption types by at least one of detecting at least one of failure of a portion of an authentication sequence or exceeding a time threshold without having detected a particular portion of the authentication sequence****.* As noted supra, Ayyagari, *et al.* and He, *et al.* are silent regarding identifying the encryption type of a wireless network by eliminating one or more of a plurality of possible encryption types based upon failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence to identify the encryption type.

In view of the foregoing, applicants' representative respectfully submits that Ayyagari, *et al.* and He, *et al.* fail to teach or suggest all limitations of independent claims 1, 21, and 22 (and claims 2-3 that depend there from), and thus fails to make obvious the subject claims. Accordingly, withdrawal of this rejection is respectfully requested

IV. Rejection of Claims 4-10, 12, 13 and 15-17 Under 35 U.S.C. §103(a)

Claims 4-10, 12, 13 and 15-17 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Ayyagari, *et al.* and He, *et al.* in further view of Krantz, *et al.* (US 2004/0111520). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Ayyagari, *et al.*, He, *et al.*, and Krantz, *et al.* do not teach each and every element of applicants' invention as recited in the subject claims.

Claims 4-10 depend from independent claim 1. As noted *supra*, Ayyagari, *et al.* and He, *et al.* do not teach or suggest each and every element of the subject invention as recited in this independent claim, and Krantz, *et al.* fails to make up for the aforementioned deficiencies of Ayyagari, *et al.* Krantz, *et al.* discloses a system for allowing a user to connect to an ISP without

requiring the user to have any previous knowledge about the requirements or have to call the ISP to connect to the ISP network. This is accomplished by redirecting the user to a URI that downloads a master document which contains information regarding the connection requirements for an ISP or by having this information pre-stored on the user's computer. In this manner, the master document is accessed to inform the user or configure the user for connection to the ISP. Krantz, *et al.* is silent regarding *a detection component that automatically* ***identifies an encryption type of an available wireless network****, wherein* ***identification of the encryption type is based at least in part upon eliminating one or more of a plurality of possible encryption types by at least one of detecting a failure of a portion of an authentication sequence of the available wireless network or exceeding a time threshold without having detected an expected portion of the authentication sequence of the available wireless network****.*

In addition, claim 4 recites ***identification of the encryption type of the available wireless network by the detection component being based, at least in part, upon iterative probing of the available network***. Contrary to assertions in the Office Action, Krantz, *et al.* fails to teach this novel feature of the subject claim. The Office Action asserts that [0066] of Krantz, *et al.* discloses this feature. However, this paragraph merely discloses that the client will send probe requests in order to identify which networks are available and then employ responses from the available beacons to identify available SSIDs and their authentication and encryption types. This authentication and encryption information is included as part of the probe response from the beacon. Each available network will send a probe response. The cited reference does not teach iterative probing of ***an*** available network in order to determine its encryption type. One probe request per network is all that is required because the beacon will respond to the probe request providing the needed information. The subject claim discloses iterative probing of a single network in order to determine the networks encryption type.

Independent claim 12 *automatically* ***identifying the encryption type of the wireless network****, wherein identification of the encryption type is based at least in part upon* ***eliminating one or more of a plurality of possible encryption types by at least one of detecting a failure of a portion of an authentication sequence or exceeding a time threshold without having detected an expected portion of the authentication sequence****, comprising:* ***attempting to connect to a wireless network as a wireless provisioning services supporting network; determining whether the attempt was successful; and, prompting for a wired equivalent privacy key, when the***

attempt was not successful. As discussed above, Ayyagari, *et al.* and He, *et al.* do not attempt to automatically identify the encryption type of a network by eliminating one or more of a plurality of possible encryption types based upon failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence to identify the encryption type. Ayyagari, *et al.* discloses that the user selects the authentication setting. Furthermore, as conceded in the Office Action, Ayyagari, *et al.* and He, *et al.* do not attempt to connect to a network using a first type of encryption (WSP) and when that is not successful employs a second type of encryption(WEP) to connect to the same network. Contrary to assertions in the Office Action, Krantz, *et al.* also fails to disclose this feature. Paragraph [0066] of the cited reference discloses that the system relies on the probe responses from beacons that inform the client of the encryption type of the wireless network associated with the beacon. The paragraph merely states that WEP is one of the encryption types as an example. Hence, the cited references fail to teach each and every feature of the subject claim.

Additionally, independent claim 15 recites ***determining whether a wireless network supports 802.1x, based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence; identifying the wireless network as an wired equivalent privacy network requiring a wired equivalent privacy key when the wireless network does not support 802.1x; determining whether the wireless network supports wireless provisioning services when the wireless network supports 802.1x based at least in part upon a failure of a portion of an authentication sequence or exceeding a time threshold during the authentication sequence; and, identifying the wireless network as an 802.1x network when the wireless network does not supporting wireless provisioning services; and, identifying the wireless network as a wireless provisioning services supporting network when the wireless network supports wireless provisioning services***. The subject claim discloses a sequential approach wherein failure of identification of one type of network is indicative of another network type. A specific narrowing sequence that checks for various network authentication types in sequential order until the authentication type of the network is identified. As previously discussed, both Ayyagari, *et al.* and Krantz, *et al.* fail to teach or suggest this novel sequence for identifying the encryption type of a wireless network. Ayyagari, *et al.* discloses that the user selects the authentication setting. He, *et al.* is silent regarding wireless networks or identification of encryption types on a wireless network. He, *et al.* merely discloses

a dial-up server switchover mechanism when the Kerberos authentication server fails. Cited pargraphs [0094 and 0098] of Krantz, *et al.* merely discloses elements of an XML file that define configuration settings for a wireless network. However, the system relies upon this XML document being download or stored on the client machine. The client machine will then employ the configuration settings to connect to the network. As such, Krantz, *et al.* relies upon the newtork to tell the client the specific encryption type being employed by the wireless network. The paragraphs do not disclose a sequence for determining the encryption type of the wireless network based upon failure of a portion of the authentication sequence or exceeding a threshold during authentication as disclosed in the subject claim.

In view of at least the foregoing discussion, applicants' representative respectfully submits that Ayyagari, *et al.*, He, *et al.* and Krantz, *et al.*, alone or in combination, fail to teach or suggest all limitations of applicants' invention as recited in independent claims 1, 12 and 15 (and claims 4-10, 13, 16 and 17 that respectfully depend there from), and thus fails to make obvious the subject claimed invention. Accordingly, withdrawal of this rejection is respectfully requested.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP552US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/
Himanshu S. Amin
Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731